

# Comment on “Quantum key distribution without alternative measurements”

Yong-Sheng Zhang, Chuan-Feng Li\*, Guang-Can Guo†

*Laboratory of Quantum Communication and Quantum Computation and Department of Physics, University of Science and Technology of China, Hefei 230026, People's Republic of China*

In a recent paper [A. Cabello, Phys. Rev. A **61**, 052312 (2000)], a quantum key distribution protocol based on entanglement swapping was proposed. However, in this comment, it is shown that this protocol is insecure if Eve use a special strategy to attack.

PACS number(s): 03.67.Dd, 03.67.Hk, 03.65.Bz

In a recent paper [1], Cabello presented a quantum key distribution (QKD) protocol based on entanglement swapping [2]. A strategy of attack by the eavesdropper (Eve) using a pair of entangled particles was discussed, and the protocol is shown to be secure in that case. However, here we will show that Eve can obtain the key without being detected by the communication parties with a pair of entangled particles.

For convenience, we use the same notation as in Ref. [1]. The four Bell states are denoted by

$$|00\rangle_{ij} = \frac{1}{\sqrt{2}} \left( |0\rangle_i \otimes |0\rangle_j + |1\rangle_i \otimes |1\rangle_j \right), \quad (1)$$

$$|01\rangle_{ij} = \frac{1}{\sqrt{2}} \left( |0\rangle_i \otimes |0\rangle_j - |1\rangle_i \otimes |1\rangle_j \right), \quad (2)$$

$$|10\rangle_{ij} = \frac{1}{\sqrt{2}} \left( |0\rangle_i \otimes |1\rangle_j + |1\rangle_i \otimes |0\rangle_j \right), \quad (3)$$

$$|11\rangle_{ij} = \frac{1}{\sqrt{2}} \left( |0\rangle_i \otimes |1\rangle_j - |1\rangle_i \otimes |0\rangle_j \right), \quad (4)$$

where  $i, j$  are labels of the particles.

The eavesdropping strategy is illustrated in Fig. 1 and can be described as follows. In the beginning, Alice has particles 1 and 2 in state  $|11\rangle_{12}$ , and 3 and 5 in state  $|10\rangle_{35}$ . Bob has particles 4 and 6 in state  $|10\rangle_{46}$ . All this information is public. Eve prepares particles 7 and 8 in state  $|10\rangle_{78}$ .

**Figure 1**

(i) Alice sends particle 2 to Bob using a public channel and makes a Bell type measurement on particles 1 and 3. Eve intercepts and keeps this particle and sends her particle 7 to Bob impersonating particle 2 Alice sends out.

(ii) Bob makes a Bell type measurement on 7 and 4, then sends particle 6 to Alice. Eve intercepts it and makes a Bell measurement on 6 and 8.

(iii) Eve makes a unitary transformation on particle 2 according to the measurement result of particles 6 and 8. She makes transformation  $I$ ,  $X$ ,  $Y$ , or  $Z$  corresponding to her measurement result  $|10\rangle$ ,  $|00\rangle$ ,  $|01\rangle$ , or  $|11\rangle$  respectively.  $I$ ,  $X$ ,  $Y$ , and  $Z$  are operators

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad (5)$$

$$Y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (1)$$

Then Eve sends particle 2 to Alice impersonating the particle 6 Bob sends out.

(iv) Alice makes a Bell type measurement on 5 and 2 and publicly announce the result. Thus Alice's and Bob's results of measurement will be consistent as if there is no eavesdropper intervening.

The reason that Eve makes a unitary operation on particle 2 is as follows. Assume that Alice's particles 2 and 5 are in state  $|\Phi\rangle$ , if Eve does not intervene and Bob's result of Bell type measurement is  $\sigma|10\rangle$  ( $\sigma$  is one of  $I$ ,  $X$ ,  $Y$  and  $Z$ ), Alice's result of Bell type measurement will be  $\sigma|\Phi\rangle$ . Now, Eve intervene the process, her result of the Bell measurement on 6 and 8 will be the same as Bob's result of the Bell measurement on 7 and 4. For the consistent of Alice's and Bob's measurement, if Eve obtain the result  $\sigma|10\rangle$ , she ought to makes a transformation  $\sigma$  on particle 2, so that when Alice measures particles 2 and 5, she obtains the proper result  $\sigma|\Phi\rangle$ .

For example, suppose that Alice obtains “11” in her measurement on particles 1 and 3, and Alice can know that the state of 5 and 2 is  $|10\rangle_{25}$ . Suppose that Bob has obtained “00” in his measurement on 7 and 4. Eve will obtain “00” in her measurement on 6 and 8 too, then she makes a transformation  $X$  on particle 2 and sends it to Alice. Alice makes a Bell measurement on 2 and 5 and will obtain the result “00”. From Table I in [1], Alice

\*Electronic address: cfli@ustc.edu.cn

†Electronic address: gcguo@ustc.edu.cn

knows that Bob has obtained “00” and Bob can know Alice’s initial result is “11”. Alice’s result “11” will be the key bits between them. Because Eve knows Bob’s result and Alice’s public announcement of the measurement result of 2 and 5, she can know Alice’s initial result “11” from Table I too.

All steps above will introduce no error in the key distribution between Alice and Bob, and Eve can know exactly the result of Bob’s measurement in step (ii) and also the public information publicly announced in step (ii). So Eve can obtain the key they distributed successfully. In conclusion, this protocol is insecure against this type attack.

This work was supported by the National Natural Science Foundation of China.

---

- [1] A. Cabello, Phys. Rev. A **61**, 052312 (2000).
- [2] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993); M. Zukowski, A. Zeilinger, M. A. Horne and A. K. Ekert, Phys. Rev. Lett, **71**, 4287 (1993); S. Bose, V. Vedral and P. L. Knight, Phys. Rev. A **57**, 822 (1998); J.-W. Pan, D. Bouwmeester, H. Weinfurter and A. Zeilinger, Phys. Rev. Lett. **80**, 3891 (1998).

**Figure caption:**

**Figure1.** Eve’s strategy to obtain Alice’s secret result. The notations are the same as in Ref. [1]. The bold lines connect qubits in Bell states, the dashed lines connect qubits on which a Bell operator measurement is made, and the pointed lines connect qubits in Bell states induced by entanglement swapping. “00” means that the bell state  $|00\rangle$  is public knowledge, (00) means that it is only known to Alice, [00] means that it is only known to Bob,  $|00|$  means that it is unknown to all the parts,  $\{00\}$  means that it is only known to Eve,  $[(00)]$  means that it is known to Alice and Bob (and Eve), etc.